IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have established an Internet-based spearphishing operation referred to as "Bohrium." Through Bohrium, Defendants are engaged in using fictitious social media profiles to obtain personal information of the victims. This in turn is used to steal credentials and break into the Microsoft accounts and computer networks of Microsoft's customers and steal highly sensitive information. To manage and direct Bohrium, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them. Internet domains used by Defendants to operate Bohrium are set forth at **Appendix A** to this Complaint and are referred to as the "Command and Control Infrastructure." Microsoft alleges as follows:

NATURE OF THE ACTION

1. This is an action based upon: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq*.; (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c) (5) Common Law Trespass to Chattels; (6) Unjust Enrichment; and (7) Conversion. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the Bohrium Command and Control Infrastructure. Defendants, through their illegal activities involving Bohrium, have caused and continue to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. On information and belief, John Doe 1 controls the Bohrium Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. On information and belief, John Doe 2 controls the Bohrium Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign

Global Registry Services (collectively, "VeriSign") are the domain name registries that oversee the registration of all domain names ending in ".com" and ".net" and are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in ".org," and is located at 1775 Wiehle Avenue, Suite 100, Reston, Virginia 20190.

7. Third party Afilias USA, Inc. is the domain name registry that oversees the registration of all domain names ending in ".info" and is located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

8. Third party Donuts Inc. is the domain name registry that oversees the registration of all domain names ending in ".live," and is located at 5808 Lake Washington Blvd NE, Suite 300, Kirkland, Washington 98033.

9. Third party DoMen is the domain name registry that oversees the registration of all domain names ending in ".me" and is located at City Kvart Masa Djurovica Lamela 3/1 Podgorica, 81000 Montenegro. DoMem is affiliated with Third party Afilias USA, Inc., located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

10. Third party XYZ.COM LLC is the domain name registry that oversees the registration of all domain names ending in ".xyz" and is located at 2121 E. Tropicana Ave Suite 2, Las Vegas, NV 89119.

11. Set forth in **Appendix A** are the identities of and contact information for third party domain registries that control the domains used by Defendants.

12. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Bohrium Command and Control Infrastructure and related infrastructure and

through those control and operate Bohrium. Microsoft will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

13. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

14. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of The Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, unjust enrichment, and

conversion pursuant to 28 U.S.C. § 1367.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

17. Defendants maintain certain of the Bohrium Command and Control Infrastructure registered through VeriSign and Public Interest Registry which reside in the Eastern District of Virginia. Defendants use these domains to communicate with and control the Bohrium-infected computers that Defendants communicate with, control, steal from, update, and maintain in this judicial district. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in and maintained through facilities in the Eastern District of Virginia, thereby injury Microsoft and its customers. Therefore, this Court has personal jurisdiction over Defendants.

FACTUAL BACKGROUND

Microsoft's Services And Reputation

18. Microsoft® is a provider of the Windows® operating system, the Outlook® email and messaging services and the Office 365® and Azure® cloud-based business and productivity suite of services. Microsoft has invested substantial resources in developing high-quality products

and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft,® Windows,® Outlook,® Office 365,® and Azure.® Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

Bohrium

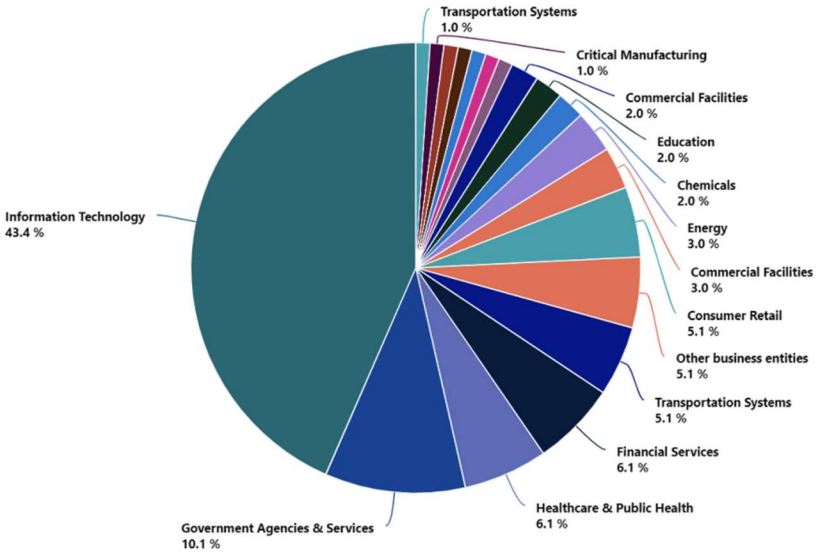
19. Bohrium specializes in spearphishing operations which are designed to steal user credentials and other sensitive information from computers connected to the Internet by infecting the targeted computers with malicious software ("malware"). The precise identities and locations of those behind the Bohrium activity are generally unknown but have been linked by many in the security community to an Iranian group or groups.

20. The Bohrium Defendants target the technology, transportation, government, and high education sectors in the Middle East, with a strong focus on the United Arab Emirates and Saudi Arabia. Bohrium also targets IT service providers, including several based in India. On information and belief, Bohrium likely targets the IT service providers to gain access to the customers that fit their victim profile.

21. Additionally, through its investigation, Microsoft has determined that Bohrium has affirmatively targeted Microsoft customers in the United States

22. Bohrium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. **Figure 1** below demonstrates that, by

sector, over half of Bohrium's targets are in the Information & Technology and Government Agencies & Services sectors. Bohrium remains an active threat today and poses a threat into the future.



23. To conduct its operation, Bohrium creates and operates fake LinkedIn Corporation ("LinkedIn")[1] profiles (profiles with fictitious names and stock image photos) to engage with targeted individuals (legitimate users of the platform) for the purpose of engaging in a tactic known as "spearphishing." Under the guise of posing as recruiting companies and claiming to help the targeted individuals obtain new employment, Bohrium operates to gain the individual's person information (such as a personal email address), and then uses that email to send the target spearphishing emails. The goal of the spearphishing emails is for the victim to download a Bohrium file that contains malware and will infect the target's computer.

[1] As of 2016, LinkedIn is a wholly owned Microsoft subsidiary. Accordingly, the harm associated with the creation of fake profiles and the use of such profiles to target legitimate users is a harm that Microsoft incurs.

24. On information and belief, Bohrium operates fake profiles that purport to be working on behalf of Freelance HR Recruiters, ApplyTalents, or Mid East Hiring, United Kingdom-based recruiting companies which specialize in hiring for Middle Eastern employers. One such fake profile that Bohrium operates purports to be "Freelance HR Recruiters," which claims to be based in the United Kingdom. Bohrium has also operated fake profiles claiming to work on behalf of ApplyTalents or Mid East Hiring. Like with Freelance HR Recruiters, ApplyTalents appears to be United Kingdom-based and also specializes in hiring for Middle Eastern employers. On information and belief, Bohrium has created a fake LinkedIn profile under the name "Roshan Sijiin."[2] This persona has been associated with the domain linkedinz[.]me, a Bohrium-controlled domain which has been used in connection with the Bohrium spearphishing operations.

25. Through the guise of recruitment efforts, Bohrium utilizes fictitious recruitment-themed profiles to target individuals in the maritime, shipping, and information technology sectors. The fictitious personas attempt to cultivate a professional rapport and encourage the target user to apply for a new job. Once the fictitious persona cultivates a professional rapport and the targeted individual is engaged, Bohrium operators then ask for the target's resume, which contains personal identifying information, including the individual's *personal email address.* On information and belief, Bohrium seeks this contact information for the purpose of moving the conversation with the target off the LinkedIn platform, so that it can continue future *email* correspondence with the target.

26. Bohrium then engages in a tactic known as "spearphishing" to compromise the account of targeted individuals. In a typical spearphishing attack, the malware sends the targeted

[2] This profile does not belong to a real user, rather it is an entirely made up profile using a fictitious name and a stock image as its profile picture. On information and belief, LinkedIn disabled this profile upon completion of the investigation.

individual an email specifically crafted to appear as if it was sent from a reputable email provider (e.g., Gmail based email addresses have been associated with Bohrium), which contains a link to a Bohrium-controlled domain. For example, the targeted individuals are sent a link to elecresearch[.]org, so that the target can begin the job application process. Because the email and link's nefarious origins are concealed, the target unsuspectingly opens the email and clicks on the link. This is typical of a spearphishing attack.

27. Bohrium then engages in a tactic known as "spearphishing" to compromise the account of targeted individuals. In a typical spearphishing attack, the malware sends the targeted individual an email specifically crafted to appear as if it was sent from a reputable email provider (e.g., Gmail based email addresses have been associated with Bohrium).

28. By gathering information about the targeted individuals from social media, public personnel directories from organizations the individual is involved with, and other public sources, Bohrium is able to package the spearphishing email in a way that gives the email credibility to the target, and makes it more likely that the target will engage with the spearphishing email. Bohrium has been observed disseminating polls asking users to identify types of software they would likely install on their device. This allows Bohrium to create an a more effective spearphishing email regarding software that the target is interested in. Similarly, Bohrium utilizes domains that either (a) impersonate legitimate companies (and trick the target into believe they are receiving legitimate communication from the impersonated company); (b) purport to provide technical, online, or cloud services (for these domains, Bohrium will send emails stating that there is a problem with the victim's account, suspicious login activity was detected, or that the target needs to download an update); or (c) utilize domains that incorporate recruitment and/or interviewing themes. Because Bohrium utilizes fake recruitment to initiate the contact, the recruitment/interviewing themed domains have been particularly successful with this category of targets.

29. The spearphishing emails often include links to websites that Bohrium has set up in advance and that it controls. When a victim clicks on the link in the email, their computer connects to the Bohrium-controlled website. For example, one domain that Bohrium has used in connection with the spearphishing operation is elecresearch[.]org or penspen[.]org , and targets are told to use this website to begin the job application process. Because the link's nefarious origins are concealed, the target unsuspectingly clicks on the link. Once the target interacts with the Bohrium-controlled domain, the target unknowingly downloads a file with malicious content. For example, when a user accesses elecresearch[.]org or another Bohrium-controlled fictitious recruitment website , the user is asked to download a file as part of the application process. In the final step of the Bohrium operation, the targets who run the file will have malicious content executed on their devices. This malicious file calls out to Bohrium-controlled infrastructure, alerting the Bohrium actors and allowing them to interact with the now-infected target machine. Here, for example, when the user runs the downloaded file, the user is presented with a short questionnaire to complete. Although the user thinks that it is filling out personal information in connection with a legitimate job posting, unbeknownst to the user, this file sends this information to an attacker C2 domain, such as microsoftdefender[.]info, sharepointfile[.]com, outlookdelivery[.]com, and microsoftsecure[.]org, which is controlled by Bohrium actors. This allows and enables Bohrium to access and control the user's device. In other instances, when the victim clicks on the link in the spearphishing email, the victim is then presented with a copy of a login page for the webmail provider that the victim is a subscriber of (*e.g.*, Hotmail, Yahoo, or Gmail). By clicking on the links contained within these spearfishing emails, the targeted user will be connected to a Bohrium-controlled website, which will attempt to induce the victim to enter their account credentials. Bohrium spearphishes targets with emails that contain a link to

an actor-controlled site intended to coerce the victim into inputting credentials or download malicious software executable onto the victim machine.

30. Once the malware, an implant, is on the victim machine, it collects clipboard data, keystrokes, and screenshots of the active window on the desktop, and then compresses and encrypts this data before writing it to a temporary file and exfiltrating these back to Bohrium's command and control infrastructure (and then server). Bohrium is able to use this data to gain access to the victims' Microsoft Office 365 accounts using the stolen credentials. Once Bohrium has access to these Microsoft Office accounts, Bohrium uses this access to steal information from these accounts. Upon successful compromise of a victim account, Bohrium frequently logs into the account from one of their IP addresses to review emails, contact lists, calendar appointments, and anything else of interest that can be found in the account. On multiple occasions, Bohrium has also created a new mailbox rule in the victim's account settings. This mailbox rule will forward all new emails received by the victim to Bohrium-controlled email addresses which are included in the auto-forward rule. In this way, Bohrium immediately receives copies of emails received by the victim, and Bohrium can store and review that stolen material on Bohrium-controlled computers, beyond the control of the victim. Bohrium also utilizes a password stealer on victim machines, allowing Bohrium to seamlessly move through other accounts using these stolen credentials. Depending on the target, in some cases, Bohrium has repeatedly targeted or attempted to target the same organization or individual over a period of months or even longer.

31. Through research and investigation, Microsoft has determined that Bohrium currently uses the domains identified in **Appendix A** to this Complaint in its command and control infrastructure. The Bohrium defendants sometimes disguise their command and control infrastructure by incorporating into the names of its command and control domains the names and

trademarks of some well-known companies and organizations, including Microsoft. As seen in **Appendix A** to this Complaint, Bohrium has registered domains that contain Microsoft's brands and trademarks as disguises. Similarly, Bohrium also uses Microsoft-Azure-based services for hosting the malicious content. Bohrium relies on the Microsoft brand and trademark to perpetrate its spearphishing and malware attacks. Bohrium's use of Microsoft services, its brand, and trademarks deceives and confuses victims into thinking that the spearphishing email is *not compromised* because the domain is Microsoft's and incorporates Microsoft's trademarks and branded material. For example, researchers or other parties who are looking for malicious activities or accidentally browse this domain may not understand that there is any malicious activity associated with it because it displays legitimate Microsoft content, which is actually displayed on a legitimate Microsoft website. Similarly, when the domain is being used for malicious purposes to target victims, the victim will be completely unaware of this fact because they are tricked into believing that the link is a legitimate Microsoft website and trustworthy, when in fact, it is malicious and actively delivering malware.

32. Bohrium's use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated with and owned by Microsoft. As noted above, by tricking victims into clicking on the fraudulent links and providing their credentials, the Bohrium defendants are then able to log into the victim's account. Additionally, the Bohrium defendants can read sensitive and personal emails within the account, create new inbox rules including auto-forwarding, access the victim's contact list, send additional spearphishing emails to the victim's contacts, and hide traces of this malicious activity in the victim account by deleting emails. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises

they work for, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

33. Once installed on a victim's computer, this malware exfiltrates information from the victim computer, maintains a persistent presence on the victim computer, and waits for further instructions from the Bohrium defendants. From there, the Bohrium defendants can send additional instructions and commands to the victim's computer, and can exfiltrate additional stolen information from that computer. By specifically targeting Microsoft's Windows operating system and utilizing registry and file paths containing Microsoft's trademarks in order to deceive users and carry out the fraudulent scheme, the Bohrium defendants infringe Microsoft's trademarks and deceptively use those trademarks in the context of Microsoft's Windows operating system.

34. The activities carried out by the Bohrium defendants, described above, injure Microsoft and its reputation, brand, and goodwill because users of compromised computers and accounts are likely to incorrectly believe that Microsoft is the source of problems caused by the Bohrium defendants. Microsoft is similarly injured because the Bohrium defendants direct their intrusions to Microsoft customer accounts hosted on Microsoft's servers and to Microsoft's Windows operating system running on customers' computers. Microsoft and its customers bear the costs of these harms. Microsoft has had to respond to customer service issues caused by the Bohrium defendants and expend substantial resources dealing with the injury and confusion and the misperception that Microsoft is the source of damage caused by the Bohrium defendants. For example, Microsoft must expend resources to block the malware discussed above, and block attempts by Bohrium to compromise user accounts. Even then, technical attempts to remedy the problem are insufficient and the injury caused to customers (and their networks and email service and internet infrastructure providers who can be targets identified through initial spearphishing

efforts) will continue.

35. Microsoft and its customers are injured when the malware used by the Bohrium defendants is maliciously introduced onto users' computers. The installation of the malware by deceived consumers and without Microsoft's authorization is an intrusion into the Microsoft Windows operating system, without Microsoft's authorization. Among other things, the Bohrium defendants install and run software without the customers' or Microsoft's knowledge or consent, to support the Bohrium infrastructure and to steal information. The Bohrium defendants specifically target the Windows operating system. For example, they write particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers, and manipulate and store data in Windows registry and file paths that contain Microsoft's trademarks. The Bohrium defendants collect and transmit personal information, including the contents of communications and files, and other personal and sensitive information from users' accounts and computers. Microsoft's customers may be incorrectly led to believe that Microsoft is the source of such issues. This causes a serious risk that customers may move from Microsoft's products and services because of the Bohrium defendants and their activities. For customers who leave, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. This causes injury to Microsoft.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

36. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 35 above.

37. Defendants knowingly and intentionally accessed and continue to access protected

computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

38. Defendants' conduct involved interstate and/or foreign communications.

39. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

40. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

41. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.*

42. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 41 above.

43. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, Outlook®, Azure®, and Office365®, among other trademarks.

44. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

45. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

46. As a direct result of Defendants' actions, Microsoft has suffered and continues to

suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

47. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq*.

THIRD CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

48. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 47 above.

49. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

50. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

51. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

52. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

53. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

54. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 53 above.

55. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

56. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

57. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

58. As a direct result of Defendants' actions, Microsoft has suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

59. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 58 above.

60. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

61. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers.

62. Defendants' actions in operating Bohrium result in unauthorized access to Microsoft's Windows operating system and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and

funds.

63. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

64. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

65. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

66. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Unjust Enrichment

67. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 66 above.

68. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

69. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

70. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

71. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

72. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

73. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Conversion

74. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 73 above.

75. Microsoft owns all right, title, and interest in its Windows software and the Outlook and Office365 software and services. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows software and its Outlook and Office365 software and services.

76. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

77. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

78. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten

profits.

79. As a direct result of Defendants' actions, Microsoft suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.

2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction giving Microsoft control over the domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.

5. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount

to be proved at trial.

8. Enter judgment awarding attorneys' fees and costs, and

9. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: May 26, 2022 Respectfully submitted,

David Ervin (VA Bar. No. 34719.)
Garylene Javier (*pro hac vice pending*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com
gjavier@crowell.com

Gabriel M. Ramsey (*pro hac vice pending*)
Anna Z. Saber (*pro hac vice pending*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
asaber@crowell.com

Attorneys for Plaintiff Microsoft Corp.